REMARKS

By this amendment, claims 1-15 are pending, in which no claim is canceled, currently amended, or newly added. No new matter is introduced.

The Office Action mailed March 6, 2006 provisionally rejected claims 1, 3, 5, 8, and 10 based on the judicially created doctrine of obviousness-type double patenting. Claims 1, 3, 5, 8, and 10 were rejected under 35 U.S.C. § 103(a) as obvious based on *Bates et al.* (US 6,785,732 B1). Further, the Office Action rejected claims 2, 4, 7, and 9 as obvious under 35 U.S.C. § 103(a) based on *Bates et al.* in view of "Network Associates Ships Cybercop Sting – Industry's first 'Decoy' Server Silently Traces and Tracks Hacker Activity" (hereinafter NAI), claims 6 and 11 as obvious under 35 U.S.C. § 103(a) based on *Bates et al.* in view of NAI and further in view of *Caccavale* (US Pub. No. 2002/0129277 A1), and claims 12-15 as obvious under 35 U.S.C. § 103(a) based on *Bates et al.* in view of NAI and further in view of *Kim et al.* (U.S. 6,701,440 B1).

The obviousness-type double patenting rejection is respectfully traversed because the two co-pending applications present claims that are patentably distinct. As an example, the following claim chart highlights some patentably distinct differences between claims 1, 3, 5, 8 and 10 of the present application and claim 1 of co-pending application 10/024,202:

Claims 1, 3, 5, 8 and 10 of present application 09/911,592	**Claim 1 of co-pending application 10/024,202**
1. (Original) A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising: a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;	1. (Original) A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising: a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code and, in response to

Claims 1, 3, 5, 8 and 10 of present application 09/911,592	Claim 1 of co-pending application 10/024,202
	detection an instance of malicious code, **generating and transmitting an event indicating the detection to a security manager**;
an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for: directing incoming electronic mail from the internet backbone to the scanning system.	an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for: directing incoming electronic mail from the internet backbone to the scanning system.
3. (Original) A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising: a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code; **a mail proxy server for determining whether the incoming electronic mail is to be scanned for malicious code** and directing the incoming electronic mail to the scanning system when the incoming electronic mail is determined to be scanned for malicious code; an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for: directing incoming electronic mail from the internet backbone to the mail proxy server.	
5. (Original) A network security system to be deployed between a plurality of intranets	

Claims 1, 3, 5, 8 and 10 of present application 09/911,592	Claim 1 of co-pending application 10/024,202
belonging to respective organizations and an internet backbone, comprising: **a plurality of scanning systems** coupled to the intranets for scanning incoming electronic mail for malicious code; **a plurality of anti-virus servers** coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; **a plurality of switches** coupled between the internet backbone, the scanning systems, and the anti-virus servers, said switches configured for: directing incoming electronic mail to at least one of the scanning systems. 8. (Original) A method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone, comprising: directing incoming electronic mail from the internet backbone to a scanning system; scanning incoming electronic mail for malicious code; and downloading anti-virus code to clients coupled to the intranets. 10. (Original) A method for maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone, comprising: directing incoming electronic mail from the internet backbone to one of a plurality of mail proxy servers; **at the one of the mail proxy servers, determining whether the incoming electronic mail is to be scanned for malicious code** and directing the incoming electronic mail to a scanning system when the incoming electronic mail is determined to be scanned for malicious code; at the scanning system, scanning incoming	

Claims 1, 3, 5, 8 and 10 of present application 09/911,592	**Claim 1 of co-pending application 10/024,202**
electronic mail for malicious code; downloading anti-virus code to clients coupled to the intranets.	

Additionally, the Office Action, on page 2, bases its rejection on the mere fact that, "the subject matter claimed in the instant application is fully disclosed in the referenced co-pending application and would be covered by any patent granted on that co-pending application since the referenced co-pending application and the instant application are claiming common subject matter." However, it has been clearly established that the co-pending applications principally underlying the double patenting rejection cannot be considered prior art against one another. *See **In re Braithwaite***, 379 F.2d 594, 154 USPQ 29 (CCPA 1967). Thus, the Office Action cites no independent evidence from which an obviousness determination can properly be based and therefore, fails to meet its initial burden of production.

Further, claim domination is an irrelevant factor. *See, e.g.*, ***In re Kaplan***, 789 F.2d 1574, 229 USPQ 678 (Fed. Cir. 1986) (holding that the mere fact that a broad claim reads on or dominates a narrower claim does not, *per se*, justify a double patenting rejection).

For at least the above reasons, the claims of the present application are patentability distinct over claim 1 of co-pending application 10/024,202.

Regarding the § 103(a) rejection to claims 1, 3, 5, 8, and 10, Applicants respectfully traverse on the merits because in Applicants' view, the present invention patentably defines over the applied art, as next discussed.

For example, independent claim 1 recites (emphasis added):

> 1. (Original) A network security system to be **deployed between a plurality of intranets** belonging to respective organizations **and an internet backbone**, comprising:
>
> a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;
>
> an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and
>
> **a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:**
>
> **directing incoming electronic mail from the internet backbone to the scanning system.**

By contrast, *Bates et al.* discloses a web server that can perform virus checking of different types of information real-time as the information is requested by a client from the web server via the Internet (Abstract; col. 3, lines 36-38). Further, Fig. 3 clearly illustrates the *Bates et al.* web server residing behind the Internet, and therefore, cannot be the claimed network security system "**deployed between a plurality of intranets** belonging to respective organizations **and an internet backbone**."

The Office Action, however, maintains (on page 3) that *Bates et al.* discloses the network security system deployed between a plurality of intranets belonging to respective organizations and an internet backbone within col. 3, lines 42-47 and col. 7, lines 23-27, that state the following (Emphasis Added):

> An example of a typical Internet connection is shown by the apparatus 200 in FIG. 2. A user that wishes to access information on the Internet 170 typically has a computer workstation referred to as a "web client" (such as web client 210B) that executes an application program known as a web browser 230. A web client, represented by 210A, 210B, and 210C in FIGS. 2 and 3, is referred to herein as a web client 210. **Under the control of web browser 230, web client workstation 210 sends a request for a web page over the Internet 170.** Web page data can be in the form of text, graphics and other forms of information, collectively known as MIME data. Each web server on the Internet has a known address, termed the Uniform Resource Locator (URL), which the web browser uses to connect to the appropriate web server. Because web server 220 can contain more than one web page, the user will also specify in the address which particular web page he wants to view on web server 220. **A web server computer system 220 executes a web server application 240, monitors requests, and services requests for which it has responsibility**. When a request specifies web server

> 220, web server application 240 generally accesses a web page corresponding to the specific request, and **transmits the web page via the Internet to the web browser 230 on the user's workstation** 210. Known web browsers include Netscape Communicator and Microsoft Internet Explorer. [col. 3, lines 41-65].
>
> Network interface 150 allows computer system 100 to send and receive data to and from any network the computer system may be connected to. This network may be a local area network (LAN), a wide area network (WAN), or more specifically the Internet 170 (as shown in FIG. 3). [col. 7, lines 23-27].

The above passages reveal that the "web clients" are individualized computer workstations and not "a plurality of intranets belonging to respective organizations." These web clients access the *Bates et al.* web server **via the Internet through network interface 150**; thus, the *Bates et al.* web server cannot be "coupled to the intranets." While the Examiner is permitted to take a reasonably broad interpretation of the claims, this doctrine does not extend to broadly reading a reference.

Despite the lack of factual support, the Office Action, on page 3, conveniently concludes "the web client can be any computer including intranet server." This statement relies not on the cited reference, but on the Examiner's own suppositions, and hence, is insufficient as a matter of law, because such conclusory statements, premised on "common knowledge and common sense," fail to fulfill requirements of the Administrative Procedure Act, ***In Re Sang Su Lee***, No. 00-1158 (Fed. Cir. Jan. 18, 2002), and that deficiencies of the cited references cannot be remedied by general conclusions about what is "basic knowledge" or "common sense." ***In Re Zurko***, 258 F.3d at 1385, 59 USPQ2d at 1697.

Additionally, the Office Action, on page 4, contends that *Bates et al.*, on col. 7, line 66 – col. 8, line 11, discloses "a **switch coupled between the internet backbone, the scanning system, and the anti-virus server**, said switch configured for: directing incoming electronic mail from the internet backbone to the scanning system." However, the Office Action subsequently contradicts this assertion stating, "Bates does not explicitly disclose a switch." The

Office Action attempts to cure the deficiency asserting that it would have been obvious to one having ordinary skill in the art to provide a connection in a distributed computing environment where multiple servers are created for each respective application. The cited passage, col. 7, line 66 – col. 8, line 22, states (Emphasis Added):

> Referring now to FIG. 4, a method 400 in accordance with the preferred embodiments allows **a virus checker on a web server to automatically check e-mail messages, web pages, and downloaded files for viruses before passing these on to a web client**. Method 400 begins when a web client requests information that normally would flow through the web server to the web client (step 410). If the request does not require virus checking (step 420=NO), the requested information is sent to the web client (step 480). If the request requires virus checking (step 420=YES), a virus check is performed on the requested information (step 430). If no virus is found (step 440=NO), the requested information is sent to the web client (step 480). If a virus is found (step 440=YES), the web client is notified of the virus (step 450), and an entry is made in the virus information database (step 460) regarding the name of the virus, type, when detected, etc. Finally, the appropriate authorities may be notified of the virus (step 470). The term "appropriate authorities" is a broad term that encompasses anyone who may need to know about the occurrence of a virus, including a network administrator of a local area network, a web site administrator, a contact person in a virus detection company, and appropriate law enforcement officials, such as local, state, federal, and international law enforcement agencies .

This passage provides no mention of a switch, much less in the manner claimed. The Office Action attempts to impose such need by asserting that "the data are re-directed to the server for checking." However, *Bates et al.* specifically states a "web server computer apparatus comprising . . . a memory . . . an e-mail server application **residing in the memory** . . . the e-mail server application having a plurality of e-mail addresses **for which it has responsibility**." Thus, the e-mail for which the web server has responsibility is not re-directed to the web server but resides thereon. If, for example, a web client had two e-mail addresses, one serviced by the *Bates et al.* web server and one not, then only the e-mail on the *Bates et al.* server would be scanned. Furthermore, since the *Bates et al.* web server is positioned behind the internet backbone, even within a distributed environment, a switch would not "direct incoming electronic mail **from the**

internet backbone to the scanning system" since the relevant data would reside on the distributed web server and be directed between components of the distributed system.

The deficiencies within *Bates et al.* cannot be cured by the addition of *Caccavale*, *Kim et al.*, or NAI. *Caccavale* is relied upon for a supposed disclosure of "performing a load-balancing procedure when there are a plurality of virus checking programs." *Kim et al.* is relied upon for providing a "sanitizing function to disinfect infected data prior to delivering data to web clients." NAI is applied for a supposed disclosure of a "decoy server used to trace and track hackers and reporting all intrusive activities."

Given that *prima facie* obviousness can only be established when all of the claim limitations are taught or suggested by the prior art, *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974), Applicants respectfully submit that a *prima facie* case of obviousness has not been established, and urge the indication that independent claims 1, 3, 5, 8, and 10 be allowed. Claims 3 and 5 are directed to a "network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone." Claims 8 and 10 recite "maintaining network security system between a plurality of intranets belonging to respective organizations and an internet backbone."

Moreover, the rejections to dependent claims 2, 4, 6, 7, 9, and 11-15 should be withdrawn, at least in part, from their dependencies from their respective independent claims 1, 3, 5, 8, and 10.

Therefore, the present application, as amended, overcomes the rejections of record and is in condition for allowance. Favorable consideration is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at (703) 425-8508 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

DITTHAVONG & MORI, P.C.

6/6/06
Date

Phouphanomketh Ditthavong
Attorney/Agent for Applicant(s)
Reg. No. 44658

10507 Braddock Road
Suite A
Fairfax, VA 22032
Tel. (703) 425-8508
Fax. (703) 425-8518